

klub paragraf 34

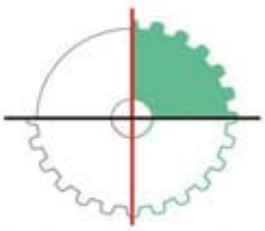
> Opis funkcji

> Przykład I

> Przykład II

Bezpieczeństwo zintegrowanych systemów sterowania – analiza przypadku automatycznego generowania dokumentacji

Wojciech Szczepka
Klub Paragraf 34

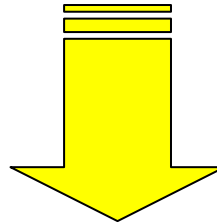


Tworzenie dokumentacji

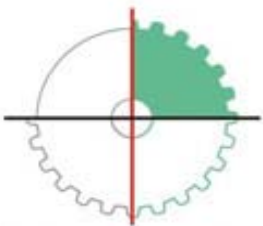
> Opis funkcji

Tworzenie dokumentacji odbywa się:

- w czasie projektowania systemu (projekt)
- podczas uruchomienia (dok. uruchomieniowa)
- podczas użytkowania systemu (urządzenia) – dokumentacja dla użytkownika



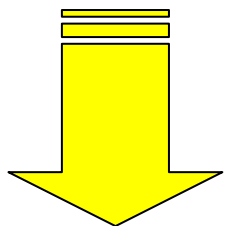
Wynikowa dokumentacja do systemu (urządzenia)



zalety automatycznego procesu wspomagania przygotowania dokumentacji

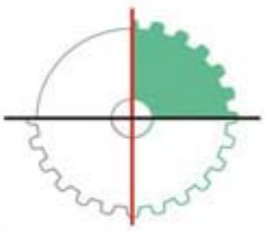
> Opis funkcji

- uniknięcie błędów (np. kopiowanie)
- zgodność ze stanem faktycznym
- brak możliwości wprowadzania nieautoryzowanych zmian
- implementacja dodatkowych funkcji testujących do całego procesu



proces generowania i podpisywania:
-plik rtf (Word)
-plik pdf

Wynik (dokument) zawsze aktualny



Przykłady:

> Opis funkcji

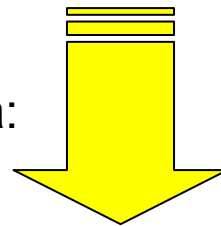
> Przykład I

> Przykład II

Przełącznik programowalny
(logiczny)



funkcje bezpieczeństwa:
•program logiczny

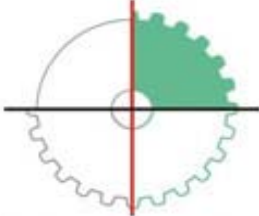


Układ sterowania
numerycznego CNC



funkcje bezpieczeństwa:
•program logiczny
+
•12 funkcji systemowych

Wynik (dokument) - zawsze aktualny



klub paragraf 34

Szablon

> Opis funkcji

> Przykład I

> Przykład II

Identification

Central unit

Order number	3RK3 111-1AA10
Short designation	3RK3 Basic
System	Modular Safety System 3RK3
Manufacturer	SIEMENS
PI profile	Safety-related devices
Device family	Safety-related devices
Device subfamily	Safety relays
Device class	Modular
Function group	0
Fieldbus interface	Not available
System interface	SAFETYconnect
Device interface	Local interface
ID no.	0
HW revision level	E01
FW revision level	V1.0.0
Revision counter	0
I&M version	1.1
Supported I&M data	1, 2, 3
Serial number	
Time stamp	5.3.2007, 14:56

Opis układu

Marking

Plant identifier	
Location identifier	
Installation date	
Description	
Author	
Comment	

Opis instalacji

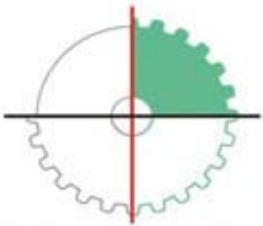
Project

Project name:	roma
Name of configuration engineer:	roman
Configuration engineer company name:	siemens
Configuration CRC:	2B879041
Configuration time stamp:	6.5.2008, 17:11
Configuration released:	No

Opis projektu

<u>Configuration CRC:</u> 2B879041			
<u>Document status:</u>			
<u>Code number</u>			
<u>Chg:</u>	<u>Version date:</u>	<u>Lang.:</u>	<u>Sheet:</u> 1/15

Diagram	Diagram name:	Diagram sheet:	Last change:	Configuration CRC:
			6.5.2008, 17:11	2B879041
Responsible Dept.:	Technical reference:	Document type:		
Owner: siemens	Created by: roman	Title: roma		
	Approved by:	Code number		
		Chg:	Version date:	Lang.:
				Sheet: 1/15



> Opis funkcji

> Przykład I

> Przykład II

Configuration of main system

MSS slot	Module	Order number	Firmware	Equipment identifier	Inputs	Outputs
2	IM PROFIBUS-DP	3RK3 511-*BA10	1.0		32	32
3	3RK3 Basic	3RK3 111-*AA10	1.0		8F	2F
4	2/4F-DI, 2F-DO	3RK3 231-*AA10	1.0		4F	2F
5	2/4F-DI, 2F-DO	3RK3 231-*AA10	1.0		4F	2F
6	2/4F-DI, 2F-DO	3RK3 231-*AA10	1.0		4F	2F

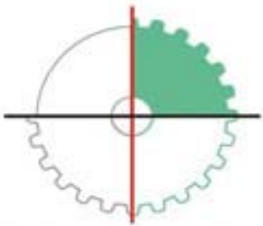
Struktura systemu (moduł główny + moduły rozszerzeń)

Configuration of main system MSS Slot 5

MSS slot 5
 Module 2/4F-DI, 2F-DO
 Order number 3RK3 231-*AA10
 Firmware 1.0
 Equipment identifier
 Inputs 4F
 Outputs 2F

opis szczegółowy

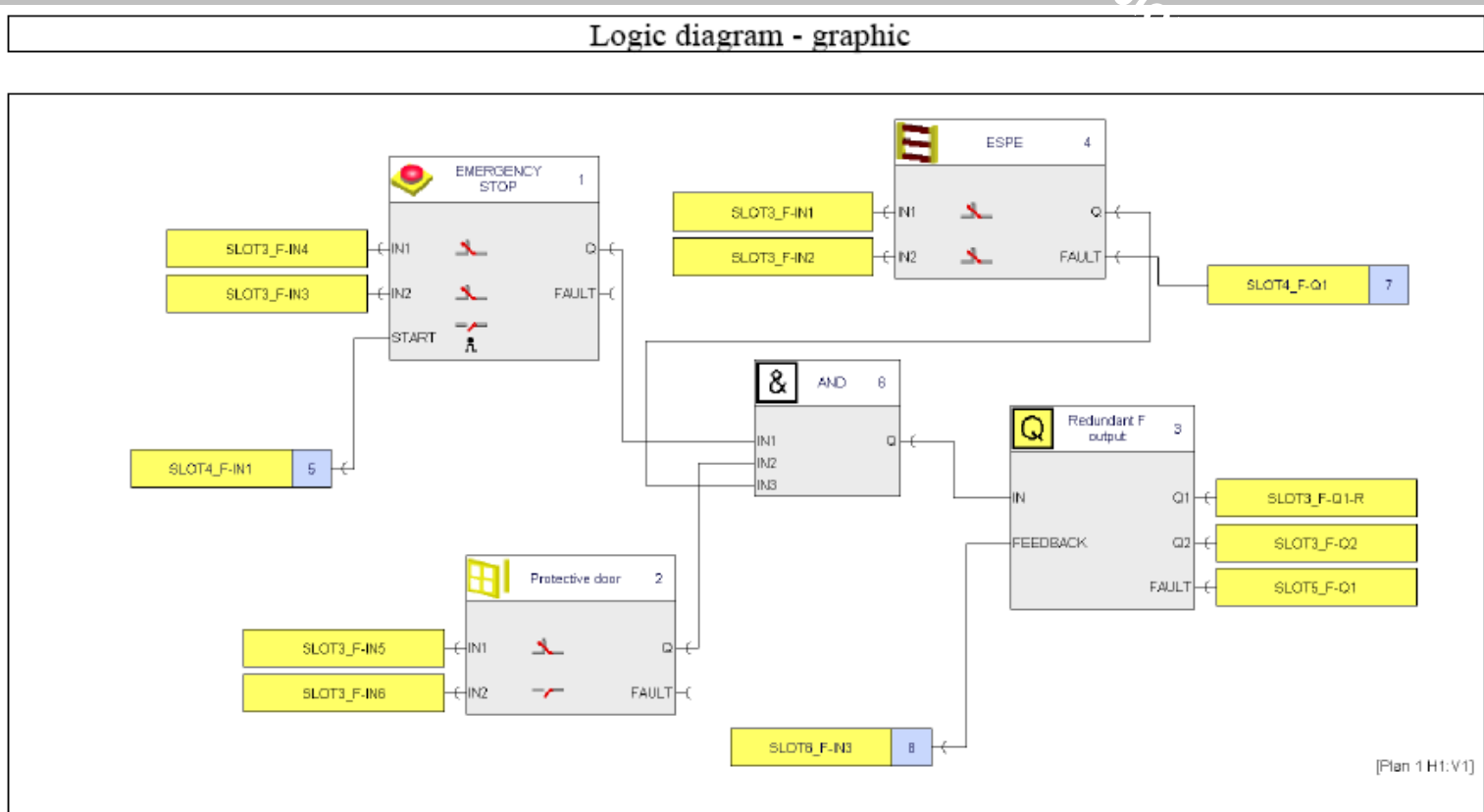
Diagram	Diagram name:	Diagram sheet:	Last change:	Configuration CRC:
			6.5.2008, 17:11	2B879041
Respons. Dept.:	Technical reference:	Document type:		Document status:
Owner:	Created by:	Title:		Code number
siemens	roman	roma		
	Approved by:	Chg.:	Version date:	Lang.:
				Sheet:
				3/15



> Opis funkcji

> Przykład I

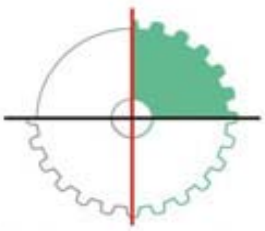
> Przykład II



[Plan 1 H1:V1]

Diagram 1/1	Diagram name: Diagram 1	Diagram sheet: 1/1	Last change: 6.5.2008, 17:11	Configuration CRC: 2B879041
Respons. Dept.:	Technical reference:	Document type:		Document status:
Owner: siemens	Created by: roman	Title: roma		Code number
	Approved by:	Chg:	Version date:	Lang: Sheet: 10/15

Schemat logiczny – wraz z edytorem

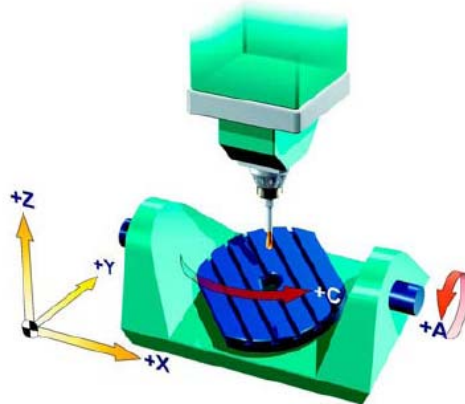


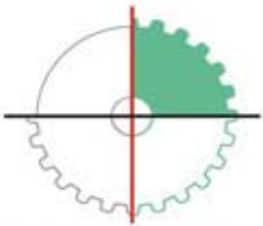
klub paragraf 34

Dodatkowe zalety w przypadku sterowań CNC

> Opis funkcji

- Maszyna pięcioosiowa (średnia ilość osi w maszynie)
- 13 funkcji bezpieczeństwa (średnio połowa jest użyta)
- Co daje $6 \cdot 5 =$ trzydzieści dokumentów
- dodatkowe procedury testujące (wykresy, funkcje zawieszenia)





Konfigurowanie testów odbiorczych

> Opis funkcji

> Przykład I

> Przykład II

The screenshot shows the CTEditor application window. The title bar reads 'CTEditor'. The menu bar includes 'Datei', 'Tätigkeit', 'Einstellungen', and 'Hilfe'. The main window is titled 'Name der Vorlage: jfhfgh'. On the left, a tree view shows the following structure:

- Informationen zur Vorlage
 - Übersicht
 - Abschaltpfad
 - Externe Stopps
 - SPL-Eingänge/Ausgänge
 - NOT-HALT
 - Funktionszusammenhänge
 - (SBH)sicherer Betriebshalt
 - SBH_1**
 - (SG)sicher reduzierte Geschwindigkeit
 - (SE)sichere Software-Endschalter

The main configuration area is for '(SBH)sicherer Betriebshalt'. It contains the following fields:

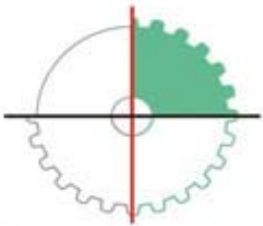
- Name: SBH_1
- Beschreibung: Hier wird der sichere Betriebshalt
- Achsanwahl: AX1:X1
- Bewegung in Positiver Richtung: Zutreffend
- Text in Übersicht/Vorgang: Allgemeine Beschreibung des Tests
- Text Schritt 1: Schritt 1
- Text Schritt 2: Schritt 2
- Text Schritt 3: Schritt 3
- Auslösebedingungen: Richtungstaste "+" auf der MSST
- Geschwindigkeits Limit: 100
- Nachlauf: 5,23
- Reaktionszeit Limit: 0
- Text für "Bestanden": Test war erfolgreich
- Text für "Nicht bestanden": Test war fehlerhaft

The right sidebar contains three sections for alarm configuration:

- Darf Nicht Auftreten**: Alarm Id: 27010 Axis: Channel: [Buttons: Alarm Hinzufügen, Alarm Entfernen]
- Muss auftreten**: Alarm Id: 123456 Axis: Channel: [Buttons: Alarm Hinzufügen, Alarm Entfernen]
- Gefiltert**: Alarm Id: 3000952 Axis: Channel: Alarm Id: 27007 Axis: Channel: [Buttons: Alarm Hinzufügen, Alarm Entfernen]

konfiguration/wyбір

parametry



klub paragraf 34

Konfigurowanie testów odbiorczych

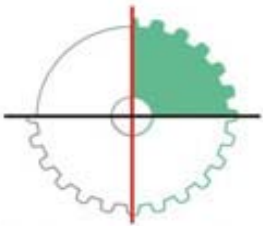
> Opis funkcji

> Przykład I

> Przykład II

Eksplorator funkcji

Opis projektu



klub paragraf 34

Konfigurowanie testów odbiorczych

> Opis funkcji

> Przykład I

> Przykład II

Test of SG (Safely Reduced Speed)
Please follow the steps listed below

Running
New Test

- 1 Select an Axis
AX1.MZ1
- 2 Select a monitoring condition
SG1
- 3 Select a direction
 Negative Positive

Monitoring of SG active: No
Selected SG override factor: None
Safe actual speed limit: None
Safe actual position: 1246.6570 mm

- 4 Press "Start Data Collection", then use JOG to move the axis so that it violates the safe speed limit.

Start Data Collection

- 5 Confirm Select
 27011 : Axis MZ1 safe velocity monitoring
 300914 : Axis MZ1 drive 1 safe velocity monitoring
 300908 : Axis MZ1 drive 1 stop C triggered
 27022 : Axis MZ1 stop C triggered

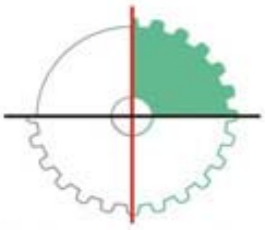
Confirm Select

< Previous Next > Finish Cancel Help

Ready

Start MMC 101/10... mmcenv runni... AccVar.exe SinuCom NC... jpeg GrafX Image... 09:14

Wbudowane przewodniki do parametryzacji testów

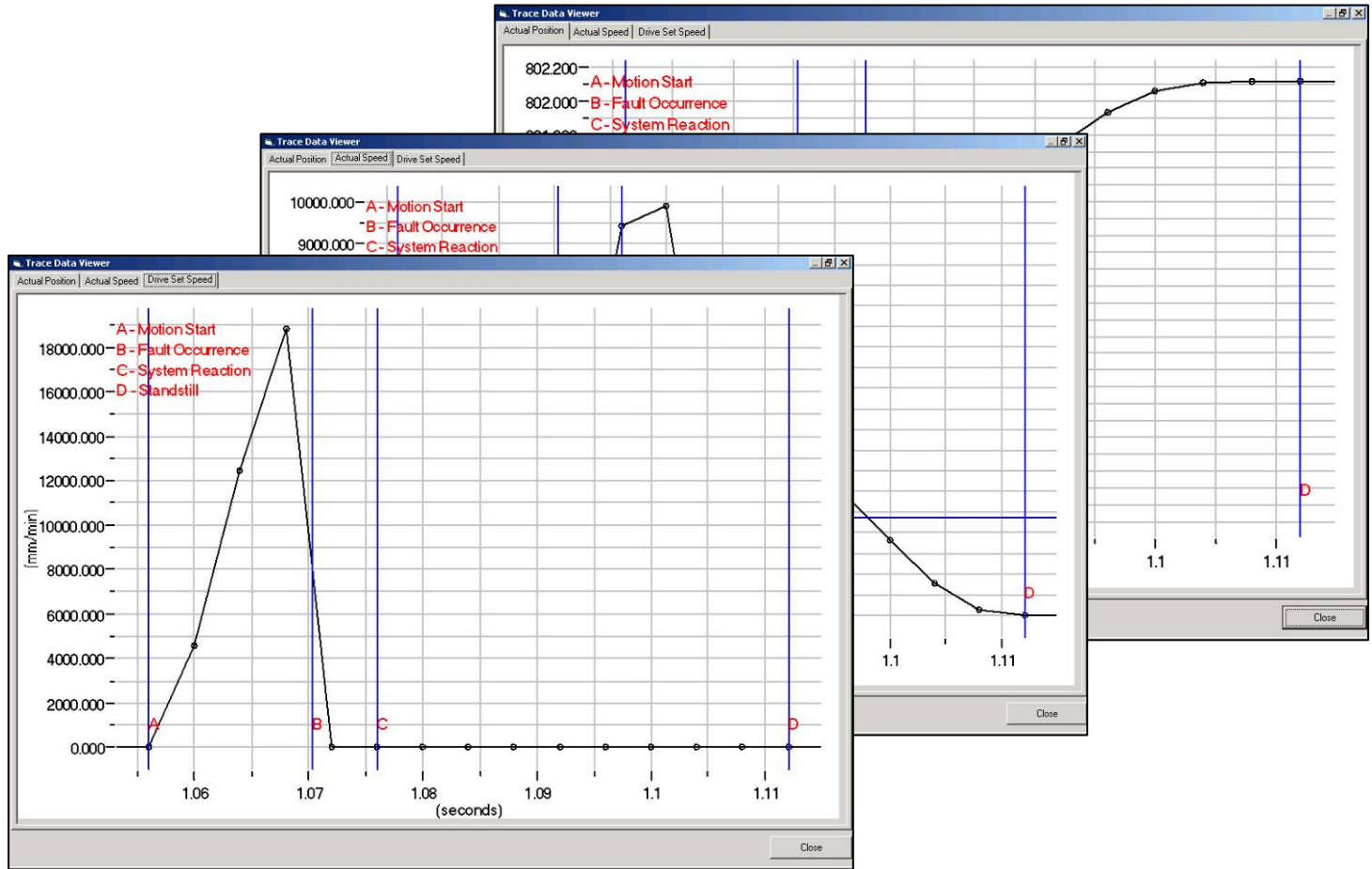


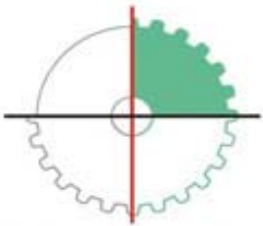
przykłady wykresów generowanych automatycznie

> Opis funkcji

> Przykład I

> Przykład II





Zabezpieczenie przed nieautoryzowaną zmianą parametrów

> Opis funkcji

> Przykład I

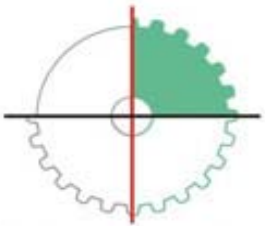
> Przykład II

Urucho- mienie	FREZARKA	JOG Ref	MPF0
Kanał RESET			Program przerwany
			ROV
Osiove dane maszynowe (\$MA_)			AX1:X1 (DR2:SRM)
36989[2]	\$MA_SAFE_CAM_MINUS_OUTPUT	0H	po
36989[3]	\$MA_SAFE_CAM_MINUS_OUTPUT	0H	po
36990[0]	\$MA_SAFE_ACT_STOP_OUTPUT	0H	po
36990[1]	\$MA_SAFE_ACT_STOP_OUTPUT	0H	po
36990[2]	\$MA_SAFE_ACT_STOP_OUTPUT	0H	po
36990[3]	\$MA_SAFE_ACT_STOP_OUTPUT	0H	po
36992	\$MA_SAFE_CROSSCHECK_CYCLE	1.056000	s po
36993[0]	\$MA_SAFE_CONFIG_CHANGE_DATE	21/11/08 14:13:31	po
36993[1]	\$MA_SAFE_CONFIG_CHANGE_DATE	04/01/94 04:12:40	po
36993[2]	\$MA_SAFE_CONFIG_CHANGE_DATE	04/01/94 03:54:18	po
36993[3]	\$MA_SAFE_CONFIG_CHANGE_DATE		po
36993[4]	\$MA_SAFE_CONFIG_CHANGE_DATE		po
36993[5]	\$MA_SAFE_CONFIG_CHANGE_DATE		po
36993[6]	\$MA_SAFE_CONFIG_CHANGE_DATE		po
36997	\$MA_SAFE_ACKN	0H	po
36998[0]	\$MA_SAFE_ACT_CHECKSUM	D14AD403H	po
36998[1]	\$MA_SAFE_ACT_CHECKSUM	0H	po
36999[0]	\$MA_SAFE_DES_CHECKSUM	D14AD403H	po
36999[1]	\$MA_SAFE_DES_CHECKSUM	0H	po
37000	\$MA_FIXED_STOP_MODE	0	po
37002	\$MA_FIXED_STOP_CONTROL	0	po

Kontrola przebiegu ruchu na twardy zderzak

↑ i >

Ogólne dane masz.	Kanał - dane masz.	Osiowe dane masz.	Widoki użytkow...		Konfigur. napędu	Dane masz. napędu
-------------------	--------------------	-------------------	-------------------	--	------------------	-------------------



klub paragraf 34

SIEMENS

Szablon

5 Attachment A1

5.1 Drive 1

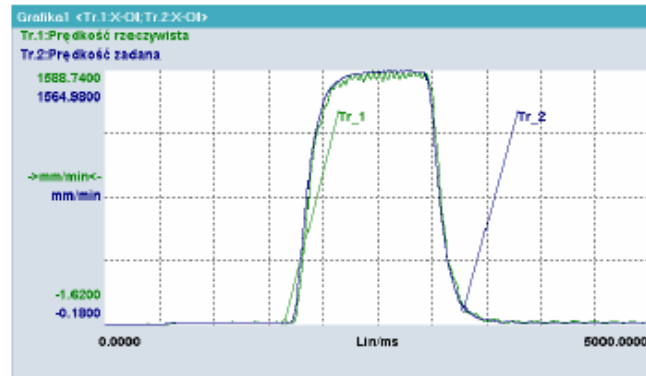


Fig. A1- 1 Testing SG1,SG2 for drive 1

5.2 Drive 2

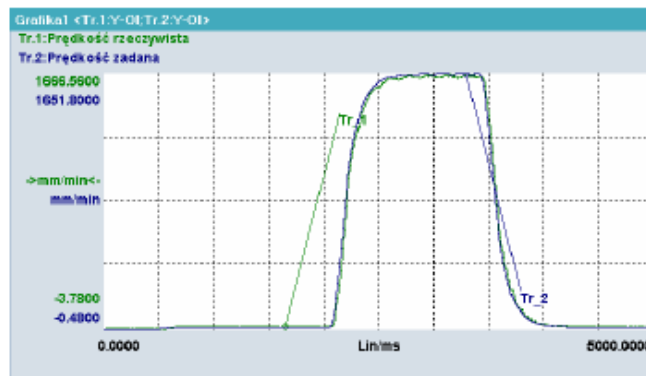
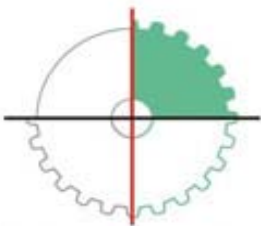


Fig. A1- 2 Testing SG1,SG2 for drive 2

> Opis funkcji

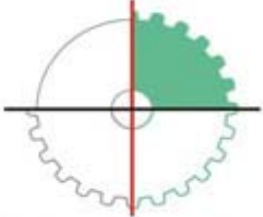
> Przykład I

> Przykład II



2.3 Safety equipment/devices

2.3.1	Przycisk „Wylączenie awaryjne” na drzwiach szafy sterowniczej. Naciśnięcie przycisku powoduje awaryjne (szybkie) zatrzymanie wszystkich napędów i wylączenie napięcia zasilania po czasie 6s.
2.3.2	Przycisk zielony podświetlany „Start” na drzwiach szafy sterowniczej. Naciśnięcie przycisku powoduje załączenie obwodów siłowych (napięcia) dla szafy sterowniczej.
2.3.3	Przycisk czerwony „Stop” na drzwiach szafy sterowniczej. Naciśnięcie przycisku powoduje wylączenie obwodów siłowych (napięcia) dla szafy sterowniczej.
2.3.4	Przycisk niebieski „Reset” Naciśnięcie przycisku powoduje odwołanie stanu „Wylączenie awaryjne”.
2.3.5	Przycisk „Wylączenie awaryjne” na pulpicie operatora. Naciśnięcie przycisku powoduje awaryjne (szybkie) zatrzymanie wszystkich napędów i wylączenie napięcia zasilania po czasie 6s.
2.3.6	Przycisk „Wylączenie awaryjne” na pulpicie sterowniczym podnośnika. Naciśnięcie przycisku powoduje awaryjne (szybkie) zatrzymanie wszystkich napędów i wylączenie napięcia zasilania po czasie 6s.
2.3.7	Przycisk „Wylączenie awaryjne” na pulpicie przenośnym operatora. Naciśnięcie przycisku powoduje awaryjne (szybkie) zatrzymanie wszystkich napędów i wylączenie napięcia zasilania po czasie 6s.
2.3.8	Przycisk „uprawnienie” na pulpicie przenośnym operatora. Przycisk naciśnięty: aktywna funkcja bezpieczne ograniczenie prędkości SG1. Przycisk nie naciśnięty: aktywna funkcja bezpieczne ograniczenie prędkości SG2.
2.3.9	Luzowniki w silnikach osi X, Y, Z, W, V, Komp. Sterowane są automatycznie poprzez program SAFE.SPF i program PLC. Aktywne gdy jest Stop A lub wylączenie regulatora pozycji dla danej osi.
2.3.10	Test stop Aktywowany ręcznie przez operatora raz na 8h pracy maszyny (przycisk na pulpicie).
2.3.11	Test luzownika osi Y Aktywowany ręcznie przez operatora raz na 8h pracy maszyny w sekwencji funkcji Test stop. (przycisk na pulpicie).
2.3.12	Bezpieczne wyłączniki krańcowe (SE) w osiach X, Y, Z, W, V. Funkcja aktywna we wszystkich trybach pracy. Aktywacja następuje przez potwierdzenie pozycji bezpiecznej przez operatora. Funkcja inicjalizowana podczas trybu „bazowania” maszyny.
2.3.13	Bezpieczny stop operacyjny (SBH) uaktywniany automatycznie poprzez program PLC i program SAFE.SPF.
2.3.14	Bezpieczne ograniczenie prędkości (SG) uaktywniane automatycznie przez program SAFE.SPF i program PLC.
2.3.15	Wyłączniki awaryjne osi posuwowych. Przejechanie wyłącznika awaryjnego jednej z osi powoduje awaryjne (szybkie) zatrzymanie wszystkich napędów i wylączenie napięcia zasilania po czasie 6s.



SIEMENS

3.1.6 Testing the EMERGENCY STOP response

EMERG STOP	Axis / spindle	Test initiated by	Braking travel Maximum speed -> standstill	Response
Szafa, pulpit, pulpit przenośny, podnośnik.	wręciono	naciśnięcie przycisku E-STOP	5s	Stop C, Stop A

Comments:

When testing the EMERGENCY STOP response, the measurement is made (braking travel with stop C). The appropriate braking travel should be taken from these measurements.

4 Completing the certificate

4.1 SI machine data

	Specified limit value checked		Attachment	
	yes	no	yes	no
Drive	X			X
NC	X			X

4.2 Check sums

4.2.1 Axis-specific

Axis / spindle		Check sum (8 HEX)			
Name	Drive number	NC MD 36998	Drive MD 1399	Time MD 36993 [0]	Date MD 36993 [0]
X	1	E98CD0C0H	11AF12H	30/11/07	04:43:04
Y	2	2968BF73CH	11A25BH	30/11/07	04:43:04
Z	3	D4E5CA67H	FC82FH	30/11/07	04:43:04
W	4	969BD62CH	FCB97H	03/12/07	06:07:19
KOMP	5	2A3C86CAH	11DA70H	03/12/07	06:07:19
V	8	C1EE14EAH	10C518H	28/11/07	00:26:04
B	9	5A3C7193H	15730DH	03/12/07	06:09:00

4.2.2 NCK-SPL (only when using SPL)

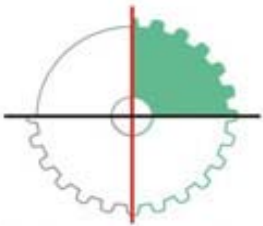
Name	Check sum (8 HEX)
SAFE.SPF	000B347DH

4.3 Completing commissioning, NCK

Name	IDS No.
11500 PREVENT_SYNACT_LOCK [0]	10
11500 PREVENT_SYNACT_LOCK [1]	105

4.4 Completing commissioning, PLC

Action	Yes
DB18.DBX36.0 statically set to "1" by the PLC program	X



4.5 Data archiving

	Memory medium			Archive location
	Type	Designation	Date	
Machine data	CD DVD		04/12/2007	Partner Serwis
PLC program	CD DVD		04/12/2007	Partner Serwis
SIMOREG DC	CD DVD		04/12/2007	Partner Serwis
Circuit diagrams	PAPER			Partner Serwis

> Opis funkcji

> Przykład I

> Przykład II

4.6 Counter-signatures

4.6.1 Acceptance test - execution

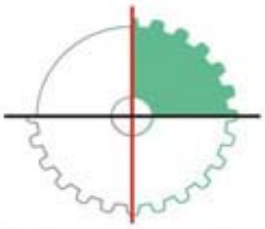
This confirms that the appropriate listed tests and checks were correctly carried-out.

Date	Name	Company/Dept.	Signature
	Wojciech Szczepka	Siemens Sp. z o.o.	

4.6.2 Counter-signed, machine OEM

Confirms the correctness of the limit values documented and specified above.

Date	Name	Company/Dept.	Signature
	Dariusz Czabon	Partner Serwis Sp. z o.o.	



klub paragraf 34

www.paragraf34.pl

> Opis funkcji

> Przykład I

> Przykład II

Dziękuję za uwagę